Präventionsstrategien

# Im Visier der Cyberkriminellen

Ob Bank, Versicherer, Industriekonzern oder Mittelständler – in der hochdigitalisierten Welt kann grundsätzlich jeder Opfer einer Cyberattacke werden. Investitionen in Cyberresilienz sollten daher heute kein Nischenthema mehr sein, sondern ein entscheidender Bestandteil jeder Unternehmensstrategie.

**Hendrik Schulze van Loon**

Banken verwalten nicht nur immense finanzielle Ressourcen. Sie verfügen auch über eine große Menge hochsensibler Daten. Gleichzeitig gehen sie im engen Gleichschritt mit der digitalen Transformation und haben systemische Bedeutung für die Wirtschaft. Dies macht sie zu einem attraktiven Ziel für Angriffe von Cyberkriminellen.

### *An erster Stelle des Risk Managements*

Am 23. Januar dieses Jahres beschrieb Mark Branson, Präsident der BaFin, bei einer Pressekonferenz die zunehmende digitale Transformation in der Finanzbranche: „Das Nervensystem der modernen Finanzwelt ist weit verästelt und hat in den vergangenen Jahren zahlreiche zusätzliche Synapsen gebildet."

Die EZB unterzieht Banken im Jahr 2024 speziellen Stresstests, um zu prüfen, wie sie auf Cyberangriffe reagieren und wie sie ihre Geschäftsbetriebe wieder herstellen können. Weiter bedeuten die im Dezember des Jahres 2022 verabschiedete NIS2-Richtlinie (NIS steht für Netzwerk- und Informationssicherheit) und der Digital Operational Resilience Act (DORA) eine Revolutionierung der Cybersicherheitsanforderungen in der gesamten EU.

Die EU-Vorgaben sehen vor, dass Unternehmen umfassende Maßnahmen im Bereich des Risikomanagements ergreifen müssen. Für Banken spielt insbesondere die DORA-Verordnung eine wesentliche Rolle (siehe auch Artikel auf Seite 73).

Die Botschaft ist klar: Die Finanzbranche muss sich anstrengen, um den Risiken der Digitalisierung gerecht zu werden. Die zunehmende Integration von Dienstleistern in die Wertschöpfungskette der Institute über digitale Schnittstellen erweitert dabei ihr Risikospektrum.

Viele Prozesse werden mit der Hilfe von externen Dienstleistern durchgeführt. Und die dortigen Sicherheitsvorkehrungen liegen oft außerhalb der Kontrolle der Institute. Kommt es dort zum Sicherheitsvorfall, kann dies auch unmittelbare Auswirkungen auf die Bank selbst haben. So wird das Risiko durch Dritte zum neuralgischen Punkt der Finanzindustrie und verdeutlicht die Bedeutung von Investitionen in die eigene Cyberresilienz.

### *Ganzheitliche Prävention*

Grundsätzlich ist keine Bank und kein Unternehmen vor Cyberangriffen gefeit. Dennoch ist es möglich, das Risiko durch strategische Krisenprävention zu minimieren. Hierzu gehören IT-seitige Penetrationstests, regelmäßige Kontrollen der IT-Infrastruktur sowie Krisenmanagement- und Krisenkommunikationsstrukturen.

Zum Ausbau der Cyberresilienz gehört darüber hinaus, sich auf den Ernstfall vorzubereiten und nach Entdeckung eines Cyberangriffs umgehend auf erfahrene Expertinnen und Experten zugreifen zu können. Denn insbesondere um großangelegte Cyberangriffe erfolgreich bewältigen zu können,

bedarf es Experten aus verschiedenen Bereichen: Krisenmanagement und Verhandlungsführung, IT-Sicherheit, Krisenkommunikation, IT-Recht und Datenschutz sowie Versicherung.

Beim letzten Punkt ist besondere Vorsicht geboten, denn Cyberversicherungen werden zu einem zunehmend riskanten Geschäft für Versicherer. In vielen Fällen ist das Risiko so hoch, dass die Deckungssummen bei Neuversicherungen in keinem sinnvollen Verhältnis mehr zu den Kosten stehen. Daher müssen Unternehmen ohne Versicherungspolice einerseits daran arbeiten, die Chance auf erfolgreiche Angriffe selbst zu minimieren. Anderseits müssen sie ebenso alles daransetzen, die Auswirkungen eines erfolgreichen Angriffs selbst möglichst gering zu halten.

Hier sind Schnelligkeit und die eingespielte Orchestrierung aller Bereiche gefragt. Dies lässt sich vor allem durch interdisziplinäre Beratungsansätze erreichen: Experten aus zentralen Bereichen der Cyberprävention können Maßnahmenpakete zur Verfügung stellen, die Prävention und 24/7-Unterstützung im akuten Krisenfall kombinieren. Sind die Bereiche eingespielt und untereinander gut vernetzt, lässt sich eine Krise schneller und effektiver managen – mit geringeren Auswirkungen auf den Geschäftsbetrieb.

### *Krisenkommunikation schafft Vertrauen*

In diesem Gefüge wird die Krisenkommunikation im Zusammenhang mit Cyberattacken oft unterschätzt. Doch in Zeiten, in denen sich Informationen schneller denn je verbreiten, entstehen auch schnell Gerüchte – und mit ihnen verbreitet sich Unsicherheit.

Kommt es zusätzlich zu einer Kompromittierung personenbezogener Daten, gilt es nicht nur, schnellstens datenschutzrechtlichen Beistand einzuholen, sondern auch, strenge Informationspflichten einzuhalten. Dann ist schnelle, transparente und zielgerichtete Kommunikation entscheidend, um das Vertrauen der Stakeholder zu erhalten.

Dementsprechend ist Krisenkommunikation einfach integraler Bestandteil von Cyberresilienz. Häufig kann effektives Kommunikationsmanagement den Unterschied zwischen einem temporären Rückschlag und einem langfristigen Reputationsschaden ausmachen.

Denn nicht zuletzt geht es darum, die kommunikative Oberhand zu behalten und den Dialog mit den Kundinnen und Kunden und den Partnerinnen und Partnern sowie der Öffentlichkeit aktiv zu gestalten. So lassen sich Professionalität und Entschlossenheit im Management von Cybervorfällen vermitteln.

### *Verantwortungsbewusst handeln*

Letztlich gilt: Treffen kann es jeden. Im Jahr 2023 wurden fast 60 Prozent aller deutschen Firmen mindestens einmal von Hackern angegriffen. Mehr Angriffe gab es nur in Irland. Das ergab eine aktuell veröffentlichte Studie des britischen Versicherers Hiscox. Im Jahr davor waren es noch knapp 45 Prozent der deutschen Firmen.

Umso wichtiger ist es, den Risiken von Cyberattacken durch Investitionen in eine moderne IT-Infrastruktur und eine ganzheitlich gedachte Sicherheitsstrategie zu begegnen. Das gilt vor allem für Bereiche, die von so großer gesellschaftlicher, wirtschaftlicher und politischer Bedeutung sind wie der Finanzsektor.

Ein interdisziplinärer Ansatz, der technische Sicherheit, rechtliche Beratung, Versicherungsschutz und Krisenmanagement sowie Krisenkommunikation miteinander verbindet, bildet eine solide Basis, um auf diese Herausforderungen zu reagieren und die digitalen Bedrohungen unserer Zeit zu bewältigen. BI

*Hendrik Schulze van Loon ist Co-Founder des Expertennetzwerks für Unternehmensresilienz Enur. Zudem ist er Managing Partner von Orca van Loon Communications sowie Dozent an der Hamburg Media School für Krisenkommunikation & Shitstorms.*

*E-Mail: hendrik.schulzevanloon@orcavanloon.de*